(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 60 977 A 1**

= US 6,839,843 B1

(51) Int. Cl.[7]:
H 04 L 9/32
G 06 F 12/14

(21) Aktenzeichen: 199 60 977.2
(22) Anmeldetag: 17. 12. 1999
(43) Offenlegungstag: 6. 7. 2000

DE 199 60 977 A 1

(30) Unionspriorität:
2256934 23. 12. 1998 CA

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Duscher, R., Dipl.-Phys. Dr.rer.nat., Pat.-Ass., 71034 Böblingen

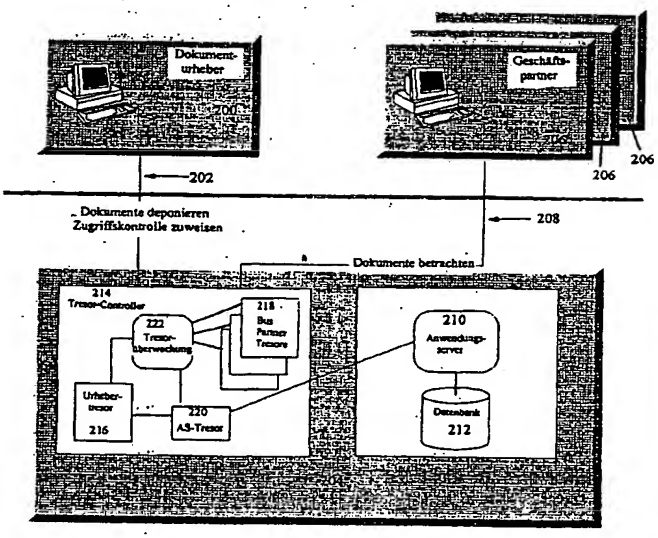
(72) Erfinder:
Bacha, Hamid, Great Falls, Va., US; Carroll, Robert Bruce, Mount Kisco, N.Y., US; Mirlas, Lev, Thornhill, Ontario, CA; Tchao, Sung Wei, Toronto, Ontario, CA

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) System für ein elektronisches Datenarchiv mit Erzwingung einer Zugriffskontrolle beim Datenabruf

(57) In einem sicheren Datenarchiv- und -austauschsystem haben sowohl der Dokumenturheber als auch der Archivverwalter Tresorumgebungen. Der Tresor des Dokumenturhebers chiffriert ein Dokument, bevor er es an den Tresor des Archivs sendet. Danach signiert der Tresor des Archivs das chiffrierte Dokument selber, bevor er das Dokument im elektronischen Archiv speichert, und sendet an den Tresor des Urhebers einen Beweis für die Deponierung. Wenn eine Einsicht in das Dokument angefordert wird, erfolgt diese Anforderung vom Tresor der anfordernden Partei an den Tresor des Archivs. Der Tresor des Archivs ruft eine Kopie des chiffrierten Dokuments ab, die er zusammen mit der Identität des Anfordernden an den Tresor des Urhebers sendet. Der Tresor des Urhebers verifiziert die Authorisierung des Anfordernden, dechiffriert dann das Dokument und sendet das dechiffrierte Dokument direkt an den Tresor des Anfordernden.



DE 199 60 977 A 1

Beschreibung

Gegenstand der Erfindung

Die vorliegende Erfindung betrifft das Gebiet der elektronischen Datenspeicherung und liefert speziell ein sicheres Datenarchiv- und -austauschsystem, das von einer dritten Partei, die die Funktion eines Verwalters ausübt, verwaltet wird, und in dem eine Zugriffskontrolle beim Abruf der Daten erzwungen wird.

Hintergrund der Erfindung

Neuere parallele Fortschritte in der Netzwerkkommunikation und der PKI-Technologie (public key infrastructure – Infrastruktur öffentlicher Schlüssel) haben bewirkt, daß Unternehmen und Institutionen beginnen, elektronische Dokumentation zur Aufzeichnung und für Transaktionen jeglicher Art einzusetzen. Mit Verbesserungen bei der Integrität und Sicherheit der Übertragung kann zuversichtlich davon ausgegangen werden, daß Dokumente, die elektronisch über das Internet und andere offene Netzwerke gesendet werden, intakt und unverfälscht ankommen.

Datenbankverwaltungssysteme, die mit modernen Computerspeichern mit einer Kapazität von mehreren Gigabyte gekoppelt sind, haben es Unternehmen und Institutionen ermöglicht, auf die Aufbewahrung von Dokumenten in Papierform zu verzichten, deren Masse Immobilienkosten verursacht.

Typischerweise müssen Daten, die von einer Stelle stammen, aus verschiedenen Gründen an eine andere übertragen werden, z. B. zur Aufbewahrung, zur Prüfung usw. Die Datenelemente könnten in Form unstrukturierter Dokumentdateien oder strukturierter Datensätze vorliegen wie z. B. Konto- und andere Finanzinformationen. Im Beispiel unstrukturierter Daten kann es notwendig sein, ein Dokument zum Zweck der Prüfung vom Ursprungssystem an andere Computer im gleichen System oder an Computer auf anderen Systemen zu schicken. Dies könnte gleichermaßen in einer Geschäftssituation (z. B. einem Vorschlag für ein Joint Venture oder einer komplexen Angebotsausschreibung) wie auch in einer Institution (z. B. wenn eine Dissertation von akademischen Beratern überprüft wird, bevor sie einer Prüfungskommission vorgelegt wird) vorkommen. Das Dokument ist elektronisch erstellt worden, da auf diese Weise Überarbeitungen und Einfügungen (speziell wenn sie umfangreich sind) leicht eingearbeitet werden können, ohne daß jedesmal das gesamte Dokument neu getippt werden muß.

Wenn das Dokument in elektronischer Form vorliegt, kann es auch leichter überprüft werden, weil es in dieser Form leichter zu übertragen ist. Anstatt das Dokument zu versenden, kann der Ersteller des Dokuments auch die vorgesehenen Prüfer wissen lassen, daß das Dokument zur Verfügung steht, und ihnen den Zugriff darauf ermöglichen. Um das Dokument zu überprüfen, muß den autorisierten Prüfern der Zugriff auf den Speicherort des Dokuments gewährt werden.

Es gibt mehrere Gründe, warum der Ersteller des Dokuments das Dokument nicht lokal speichern möchte. Wenn die lokale Speicherung des Dokuments bedeutet, daß hinter der Firewall anderen Stellen offener Zugriff gewährt wird, besteht ein Sicherheitsrisiko (die Gefahr von Hackerangriffen). Der Zugriff auf den lokalen Speicher stellt auch eine Gefahr für die Datenverwaltung dar, da eine einzige unbedachte Aktion von einem Prüfer die Dokumentdatei löscht. Auch kann mangelnde Verfügbarkeit des Systems und/oder des Netzwerks mögliche Vorteile, die ein Prüfer darin sieht,

daß ihm direkter Zugriff auf das Dokument im Speicher gewährt wird, zunichte machen. Die Systemverfügbarkeit gibt an, ob der lokale Computer oder das LAN des Urhebers des Dokuments jederzeit für Prüfer zugänglich ist, und die Netzwerkverfügbarkeit bezeichnet die Einschränkung, daß es für das Netzwerk schwierig sein kann, mehrere Punkte dem lokalen Speicherort zur Verfügung zu stellen, wenn mehrere Prüfer gleichzeitig zugreifen wollen.

In einer Geschäfts- oder Institutionssituation könnte es auch Gründe dafür geben, daß eine unabhängige Verifizierung notwendig ist, um nachzuweisen, daß ein Urheber eines Dokuments dieses an einem bestimmten Datum vorgelegt hat (z. B. ein kommerzielles Angebot).

Eine Lösung besteht darin, das Archiv einer dritten Partei zu nutzen, und zwar speziell einer Partei, deren Zweck es ist, den Dienst einer sicheren Datenarchivierung anzubieten, und die bei Bedarf einen Deponierungsbeweis erbringen kann.

In den US-Patentschriften Nr. 5,615,268 und 5,748,738, beide mit dem Titel "System and Method for Electronic Transmission Storage and Retrieval of Authenticated Documents" und beide der Document Authentication Systems, Inc. übertragen, wird ein System beschrieben, das Datenintegrität und Deponierungsbeweis mit Hilfe eines Windows-Client zur Kommunikation mit den Datenspeicherdateien anbietet.

Eine wichtige Überlegung, die in diesen Patentschriften nicht angesprochen wird, ist, daß die Integrität der im Archiv gespeicherten Daten und der Zugriff auf diese Daten nicht von den Aktionen der dritten Partei, die das Dokumentarchiv verwaltet, abhängig sein darf. Anders ausgedrückt, der Datenverwalter darf nicht in der Lage sein, unabsichtlich oder böswillig den Inhalt der Daten zu verändern, ohne daß dies von den Systembenutzern bemerkt wird. Außerdem darf es dem Datenverwalter nicht möglich sein, das Zugriffsrecht oder die Verweigerung des Zugriffsrechts eines Benutzers auf ein Datenelement zu ändern.

In dem genannten System der US-Patentschriften 5,615,268 und 5,748,738 wird darauf vertraut, daß der Datenarchivservice die Daten nicht für andere Benutzer einsehbar macht. In diesem System gibt es keine Vorkehrungen, die die Vertraulichkeit der Daten mit Hilfe der Verschlüsselungstechnologie gewährleistet.

Kurzbeschreibung der Erfindung

Es ist deshalb eine Aufgabe der vorliegenden Erfindung, ein System zur elektronischen Speicherung und zum elektronischen Austausch von Dokumenten zur Verfügung zu stellen, in dem die Dokumente physisch in einem von einer dritten Partei verwalteten Archiv gespeichert werden, in dem die Benutzer aber auf ihre Dokumente zugreifen und sie mit anderen gemeinsam benutzen können.

Eine weitere Aufgabe der Erfindung besteht darin, ein System zur Verfügung zu stellen, in dem die Integrität der im Archiv gespeicherten Daten und der Zugriff darauf nicht von den Aktionen der dritten Partei, die das Archiv verwaltet, abhängig ist.

In einem Aspekt hat die vorliegende Erfindung also ein sicheres elektronisches Datenspeicherungs- und -abrufsystem zum Ziel, das aus einem Datenarchiv, einem Datenarchiv-Verwalter, der Speicherung und Abruf verschlüsselter elektronischer Daten eines das Dokument deponierenden Computers in das und aus dem Archiv verwaltet, und einem Agentenprogramm des zur Speicherung verwendeten Computers besteht. Das Agentenprogramm ist für den Archiv-Verwalter immer zugänglich, unabhängig davon, ob der Computer online oder offline arbeitet. Das Agentenpro-

gramm besitzt auch Mittel, um nach Authentifizierung eines anfordernden Computers die verschlüsselten elektronischen Daten des deponierenden Computers, die auf Anfrage des anfordernden Computers aus dem Datenarchiv abgerufen werden, zu dechiffrieren. Vorzugsweise kann der Archivverwalter die chiffrierten elektronischen Daten mit einer digitalen Signatur versehen, bevor sie im Datenarchiv gespeichert werden, und dann eine Kopie der mit der Signatur versehenen chiffrierten Daten an das Agentenprogramm senden, so daß das Agentenprogramm nach der Dechiffrierung anhand der signierten chiffrierten Daten die abgerufenen chiffrierten elektronischen Daten überprüfen kann.

In einem anderen Aspekt liefert die vorliegende Erfindung ein System und ein Verfahren zur sicheren Authentifizierung des Benutzerzugriffs auf elektronische Daten, die in einem Datenarchiv gespeichert sind, das von einem Archiv-Verwalter verwaltet wird, der mit der Quelle der Daten nichts zu tun hat, wobei den elektronischen Daten bei der Speicherung im Datenarchiv eine Zugriffskontroll-Liste der Benutzerzugriffsberechtigungen zugeordnet wird. Die Quelle ist für die Aktualisierung der Zugriffskontroll-Liste zuständig und erbringt Nachweis der aktuellen Zugriffskontroll-Liste. Der Nachweis der aktuellen Zugriffskontroll-Liste wird auch jedem Benutzercomputer, der die Aktualisierung vorgenommen hat, zur Verfügung gestellt.

Die Quelle überprüft, bevor sie die Daten für den anfordernden Computer freigibt, ob die aktualisierte Zugriffskontroll-Liste, die mit den elektronischen Daten im Datenarchiv gespeichert ist, korrekt ist.

Die Verwendung der Erfindung ist besonders vorteilhaft in einem System mit einer großen Anzahl von Dokumenten, die von einer großen Anzahl von Benutzern benutzt werden können und benutzt werden. Die Zentralisierung der Benutzerzugriffsdaten verbessert die Systemeffizienz, da auf diese Weise eine Duplikation der Information vermieden wird. Außerdem ermöglicht die Verwendung einer mächtigen, zentralisierten Suchautorität eine umfangreichere Suche – Parameter müssen nicht auf die Dokumentidentität beschränkt sein, sondern können möglicherweise andere Identifikationsdaten enthalten, z. B. die Erstellungszeit, die Identität des Dokumenturhebers usw.

Die Erfindung kann in Form von Datenträgern, die mit Programmcode codiert sind, realisiert werden, um das oben beschriebene System oder die beschriebenen Verfahren zu realisieren.

Kurzbeschreibung der Zeichnungen

Im folgenden werden Ausführungsbeispiele der Erfindung ausführlich in Verbindung mit den beigefügten Zeichnungen beschrieben. Die Zeichnungen haben folgenden Inhalt:

Fig. 1 ist eine Schemazeichnung von einem Dokumentarchivsystem, das von einer dritten Partei verwaltet wird.

Fig. 2 ist eine Schemazeichnung, ähnlich wie **Fig.** 1, in der ein Tresor-Dokumentarchivsystem dargestellt ist, das in der bevorzugten Ausführungsform der vorliegenden Erfindung verwendet wird.

Fig. 3 ist ein Flußdiagramm des Dokumenterstellungsverfahrens gemäß der Erfindung.

Fig. 4, bestehend aus **Fig.** 4A und **Fig.** 4B ist ein Flußdiagramm des Dokumentabrufverfahrens gemäß der Erfindung.

Fig. 5 ist ein Flußdiagramm eines Verfahrens, gemäß der bevorzugten Ausführungsfarm der Erfindung, das für die Unveränderlichkeit der Zugriffskontrolle für den Dokumentabruf sorgt.

Fig. 6 schließlich ist ein Flußdiagramm eines erfindungsgemäßen Verfahrens zur Zuordnung von Eignerzugriffsrechten auf gespeicherte Dokumente.

Ausführliche Beschreibung der bevorzugten Ausführungsformen

Eine konventionelle Anordnung für ein Dokumentarchivsystem, bei dem eine dritte Partei als Verwalter agiert, ist in **Fig.** 1 dargestellt. Ein Dokumenturheber **100** kann Dokumente über seine Verbindung **102** mit einem fernen Dokumentarchivdienst **104**, z. B. einer von einer dritten Partei verwalteten Datenbank, deponieren. Als Eigner der deponierten Dokumente kann der Urheber **100** Zugriffsrechte auf die Dokumente zuweisen. Der Urheber eines Dokuments kann beispielsweise festlegen, daß ein Geschäftspartner **106** die "Lese"-Berechtigung hat, d. h. daß er das Dokument über seine Verbindung **108** mit dem Dokumentarchivdienst **104** abrufen, aber nicht ändern darf.

In solchen konventionellen Systemen ist das vom Urheber **100** deponierte Dokument normalerweise nicht verschlüsselt, so daß der Geschäftspartner **106** das Dokument auf Verlangen prüfen kann. Der Grund dafür ist, daß es nach dem Stand der Technik Probleme mit der Dechiffrierung von Dokumenten gibt. Für die Dechiffrierung eines Dokuments ist der Zugriff auf den privaten Schlüssel des Dokumenturhebers **100** erforderlich. Um den Zugriff auf seinen privaten Schlüssel zu ermöglichen, muß der Dokumenturheber **100** entweder selber zu allen Zeiten, zu denen möglicherweise eine Dechiffrierung angefordert werden könnte, online erreichbar sein, um die Dechiffrierung selber vorzunehmen (die Frage der Systemverfügbarkeit), oder er muß im voraus einen Plan entwickeln, um seinen privaten Schlüssel dem Geschäftspartner **106** direkt oder über einen vertrauenswürdigen Proxy-Server (nicht dargestellt) zukommen zu lassen.

In der US-Patentschrift Nr. 5,491,750 der International Business Machines Corporation, mit dem Titel "Method and Apparatus for Three-Party Entity Authentication and Key Distribution Using Message Authentication Codes", wird ein System beschrieben, das die Verteilung geheimer Sitzungsverwaltungsschlüssel ermöglicht, die von zwei oder mehr Kommunikationspartern gemeinsam benutzt werden können, nachdem die Kommunikationspartner durch einen vertrauenswürdigen Vermittler authentifiziert worden sind. Die so erzeugten Schlüssel und andere ähnliche sind aber kurzlebig und ihre Verwendung sollte auf das absolut Notwendige beschränkt werden. Es ist nicht klar, daß ein solches Konzept geeignet wäre, Dechiffrierschlüssel in einem Dokumentrevisionssystem mit einem dauerhaften Dokumentarchiv sicher zwischen Kommunikationspartnern zu übertragen.

In konventionellen Systemen, in denen Dokumente für einige Zeit deponiert werden und nicht chiffriert sind (**Fig.** 1), muß darauf vertraut werden, daß die dritte Partei, die den Archivdienst **104** verwaltet, die Integrität des Dokuments bewahrt.

Das Dokumentarchivsystem in der bevorzugten Ausführungsform der vorliegenden Erfindung ist mit dem Produkt IBM Vault Registry erstellt, das Gegenstand der US-Patentanmeldung Nr. 980,022 mit dem Titel "Secure Server and Method of Operation for a Distributed Information System", eingereicht am 26. November 1977 und der IBM Corporation übertragen, ist. Die US-Patentschrift Nr. 980,022 ist hiermit durch Bezugnahme Teil des vorliegenden Dokuments. Das Produkt IBM Vault Registry bietet eine erweiterte Webserver-Umgebung, die eine sichere Erweiterung, einen sogenannten Tresor, der Klientenumgebung implementiert. Dieses System vertraut auf die im Hintergrund der Erfindung beschriebene moderne Übertragungstechnologie,

genden Erfindung kcinnte es sich dabei auch um ACL- und Fähigkeitslisten-Aktualisierungen handeln. Wenn dies geschieht, stimmen die auf den Benutzerarbeitsplätzen gespeicherten Verifizierungstokens möglicherweise nicht mehr mit den Tokens in den entsprechenden Tresoren überein, so daß die Benutzer keinen Zugriff mehr haben.

Deshalb wurde als Standard für die Datenwiederherstellung in verschiedenen Situationen das folgende System implementiert. Es wird angenommen, daß die Sicherung zum Zeitpunkt ZEIT1 erfolgte, während die Rückspeicherung zu einem späteren Zeitpunkt ZEIT2 mit dem Stand der Daten zum Zeitpunkt ZEIT1 stattfand, an dem der Anfordernde das Dokument abgerufen hat.

Wenn eine vollständige Rückspeicherung der Dokumentdatenbank, der ACLs, der Fähigkeitslisten und der entsprechenden in den Tre oren gespeicherten Tokens durchgeführt wird, können die Benutzer, die vor ZEIT1 auf ein Dokument zugreifen konnten, dies auch nach ZEIT2 tun. Dies bedeutet, daß wenn ein Benutzer vor ZEIT1 berechtigt war, die Berechtigung aber zwischen ZEIT1 und ZEIT2 widerrufen wurde, dieser Benutzer dennoch auf das Dokument zugreifen kann, bis der Urheber des Dokuments das ACL-Token prüft. Nach einer vollständigen Datenrückspeicherung sollten deshalb alle Benutzer eine Prüfung der ACL und der Fähigkeitsliste durchführen.

Wenn nur die Dokumentdatenbank zurückgespeichert wurde und die ACLs, die Fähigkeitslisten und die in den Tresoren gespeicherten Tokens unberührt geblieben sind, können Benutzer feststellen, daß sie das Zugriffsrecht für ein Dokument besitzen, das gar nicht in der Datenbank gespeichert ist, da das Dokument nach ZEIT1 hinzugefügt wurde, aber nachher bei der Rückspeicherung der Datenbank verloren gegangen ist. Da alle Tokens aktuell sind, gibt es keine weiteren Anomalien.

Ein anderer Fall liegt vor, wenn in einem System keine Fähigkeitslisten benutzt werden, die ACLs aber in der Anwendungsdatenbank gespeichert werden. Wenn die Dokumentdatenbank und die ACL zurückgespeichert worden sind, während die in den Tresoren gespeicherten Tokens nicht zurückgespeichert wurden, stellen die Benutzer fest, daß alle Dokumente, deren ACL nach ZEIT1 geändert wurden, nicht mehr zugänglich sind. Dies kommt daher, daß die ACL-Tokens in der Anwendungsdatenbank nicht mit den in den Tresoren der einzelnen Eigner gespeicherten Tokens übereinstimmen. Um dieses Problem zu lösen, müssen alle Dokumenturheber die ACLs aktualisieren. Eine Möglichkeit dazu ist, daß der Verwalter die alten ACLs (die zu ZEIT1 in Kraft waren), den Dokumenturhebern sendet und sie bittet, die entsprechenden Tokens in ihren Tresoren neu zu installieren. Diese Aktualisierung wird manuell, nicht automatisch, vorgenommen, und die Dokumente eines Eigners sind unzugänglich, bis er die Aktualisierung durchgeführt hat.

In Situationen, in denen Datenbankinkonsistenzen vermieden werden müssen, kann der Archivverwalter nach einer Rückspeicherung den Zugriff auf alle Dokumente sperren, bis der Urheber Fehlerbehebungsmaßnahmen ergriffen hat. Diese Sperre kann für alle Dokumente im Archiv gelten oder nur für einen Teil der Dokumente, bei denen die Konsistenz am kritischsten ist. In diesem Fall muß man sich auf den Archivverwalter verlassen, um die Konsistenz des Systems zu wahren. Wie bereits erwähnt hat der Verwalter aber in keinem Fall die Möglichkeit, Benutzerzugriffsrechte auf ein Dokument zu erteilen oder zu widerrufen.

Um die Möglichkeit einer konzertierten Attacke auf das System zu minimieren, ist es wichtig, daß die Rollen zwischen dem Verwalter des Tresorservers und des betreffenden lokalen Tresorspeichers einerseits und dem Datenbankverwalter andererseits getrennt sind.

In der obigen Beschreibung wurden bevorzugte Ausführungsformen der vorliegenden Erfindung mittels des Produkts IBM Vault Registry beschrieben. Dem Fachmann ist aber klar, daß die vorliegende Erfindung auch mit anderen Produkten, die über ähnliche Funktionen verfügen, implementiert werden könnte, z. B. mit sicheren tresorähnlichen Umgebungen, die sich lokal auf dem Arbeitsplatz der einzelnen Benutzer befinden. Solche und andere Abwandlungen, die für den Fachmann offensichtlich sind, sollen ebenfalls unter den Schutzumfang der beigefügten Ansprüche fallen.

Patentansprüche

1. Ein sicheres elektronisches Datenspeicherungs- und -abrufsystem, umfassend:
ein Datenarchiv;
einen Archivverwalter zur Verwaltung der Speicherung und des Abrufs von chiffrierten elektronischen Daten eines deponierenden Computers in dem und aus dem Datenarchiv;
ein Agentenprogramm des deponierenden Computers, auf das der Archivverwalter zugreifen kann, unabhängig davon, ob der deponierende Computer online oder offline arbeitet, und das Mittel besitzt, um nach Authentifizierung des anfordernden Computers die chiffrierten elektronischen Daten des deponierenden Computers, die auf Anforderung des anfordernden Computers aus dem Datenarchiv abgerufen werden, zu dechiffrieren.

2. Das System nach Anspruch 1, wobei der Archivverwalter außerdem daran angepaßt ist, die chiffrierten elektronischen Daten vor der Speicherung im Datenarchiv mit einer digitalen Signatur zu versehen und eine Kopie der signierten chiffrierten Daten an das Agentenprogramm des deponierenden Computers zu senden, und wobei das Agentenprogramm des deponierenden Computers daran angepaßt ist, anhand der signierten chiffrierten Daten die abgerufenen chiffrierten Daten nach der Dechiffrierung zu verifizieren.

3. Das System nach Anspruch 1 oder 2, wobei das Agentenprogramm außerdem daran angepaßt ist, die dechiffrierten elektronischen Daten an den anfordernden Computer zu senden.

4. Das System nach Anspruch 3, wobei das Agentenprogramm eine sichere Erweiterung des deponierenden Computers ist und daran angepaßt ist, die Kommunikation zwischen dem deponierenden Computer und dem Archivverwalter zu verwalten.

5. Das System nach Anspruch 4, das außerdem einen Server umfaßt, der Kommunikationsverbindungen mit dem Archivverwalter, den deponierenden Computer und dem anfordernden Computer besitzt, und der folgendes enthält:
das Agentenprogramm des deponierenden Computers;
eine zweite Umgebung, die eine sichere Erweiterung des Archivverwalters umfaßt, und die daran angepaßt ist, Übertragungen von und zu anderen Umgebungen auf dem Server mit dem Archivverwalter zu verwalten; und
mindestens eine dritte Umgebung, die eine sichere Erweiterung des anfordernden Computers umfaßt, und die daran angepaßt ist, Übertragungen von und zu anderen Umgebungen auf dem Server mit dem anfordernden Computer zu verwalten.

6. Das System nach Anspruch 4 oder 5, wobei das Agentenprogramm des deponierenden Computers Mit-

tel zum Chiffrieren und digitalen Signieren der vom deponierenden Computer empfangenen elektronischen Daten und zum senden der chiffrierten elektronischen Daten und der Signatur an den Archivverwalter zur Speicherung im Datenarchiv umfaßt.

7. Ein Prozeß zur sicheren Authentifizierung des Benutzerzugriffs auf elektronische Daten, die in einem von einem Archivverwalter, der nichts mit einer Quelle der elektronischen Daten zu tun hat, verwalteten Archiv gespeichert sind, umfassend:
Zuordnen einer Zugriffskontroll-Liste der Benutzerberechtigungen für die elektronischen Daten bei Speicherung im Datenarchiv;
Durchführung von Aktualisierungen der Zugriffskontroll-Liste von der Quelle der elektronischen Daten aus;
Speichern der aktualisierten Zugriffskontroll-Liste mit den im Datenarchiv gespeicherten elektronischen Daten;
Speichern eines Beweises der aktualisierten Zugriffskontroll-Liste an der Quelle der elektronischen Daten und auf jedem Benutzercomputer, der die Aktualisierung durchgeführt hat; und
Verifizieren der Richtigkeit der mit den elektronischen Daten im Datenarchiv gespeicherten Zugriffskontroll-Liste mit einem an der Quelle gespeicherten Beweis, bevor die elektronischen Daten für einen anfordernden autorisierten Benutzer freigegeben werden.

8. Der Prozeß nach Anspruch 7, wobei der Schritt der Durchführung von Aktualisierungen an der Zugriffskontroll-Liste folgendes umfaßt:
Identifizieren einer Revisionsstufe der aktualisierten Zugriffskontroll-Liste; und
Zuordnen eines aktuellen Zeitstempels zu der aktualisierten Zugriffskontroll-Liste,
und wobei der Schritt der Beweisspeicherung folgendes umfaßt:
Erstellen eines Tokens der Revisionsstufe und des aktuellen Zeitstempels; und
Speichern des Tokens bei jedem Benutzer mit Zugriffsrecht auf die elektronischen Daten im Datenarchiv.

9. Der Prozeß nach Anspruch 8, außerdem umfassend:
Anhängen des Tokens an die aktualisierte Zugriffskontroll-Liste, um eine Datenstruktur zu bilden;
digitale Signierung der Datenstruktur; und
Speichern der signierten Datenstruktur mit der aktuellen Zugriffskontroll-Liste im Datenarchiv und an der Quelle, und wobei der Schritt der Verifizierung der Richtigkeit der aktualisierte Zugriffskontroll-Liste folgendes umfaßt:
Verifizieren der Dechiffrierung der Datenstruktursignatur an der Quelle; und
Vergleichen der verifizierten Datenstruktur mit der aus dem Datenarchiv abgerufenen aktualisierten Zugriffskontroll-Liste.

10. Der Prozeß nach Anspruch 8, wobei der Schritt der Beweisspeicherung außerdem folgendes umfaßt:
digitale Signierung des Tokens; und
Speichern des signierten Tokens an der Quelle.

11. Der Prozeß nach Anspruch 10, außerdem umfassend:
Senden des digital signierten Tokens an einen von der Quelle zur Aktualisierung der Zugriffskontroll-Liste autorisierten Benutzers; und
bei Vorlegen des digital signierten Tokens durch den zur Aktualisierung der Zugriffskontroll-Liste berechtigten Benutzer,
Verifizierung der Tokensignatur an der Quelle; und
Vergleichen des verifizierten Tokens mit der Revisionsstufe und dem aktuellen Zeitstempel, die der aus dem Datenarchiv abgerufenen aktualisierten Zugriffskontroll-Liste zugeordnet sind.

12. Ein Verfahren zum sicheren Speichern und Abrufen elektronischer Daten in einem fernen Datenarchiv, umfassend:
digitales Signieren der elektronischen Daten an der Quelle;
Chiffrieren der elektronischen Daten an der Quelle;
Senden der chiffrierten elektronischen Daten an das Datenarchiv;
digitales Signieren der chiffrierten elektronischen Daten im Datenarchiv, um einen Deponierungsbeweis zu erzeugen;
Speichern der chiffrierten elektronischen Daten und des Deponierungsbeweises im Datenarchiv; und
Zurücksenden einer Kopie des Deponierungsbeweises an die Quelle.

13. Das Verfahren nach Anspruch 12, außerdem umfassend:
Empfangen einer Zugriffanforderung auf die gespeicherten elektronischen Daten von einem anfordernden Benutzer;
Abrufen der chiffrierten elektronischen Daten und Senden der abgerufenen Daten an die Quelle;
Verifizieren des anfordernden Benutzers als zum Zugriff auf die elektronischen Daten Berechtigen; und
falls verifiziert, Dechiffrieren der abgerufenen Daten.

14. Das Verfahren nach Anspruch 13, außerdem umfassend:
Zuordnen einer Zugriffskontroll-Liste der Benutzerberechtigungen für die elektronischen Daten bei Speicherung im Datenarchiv;
Durchführung von Aktualisierungen der Zugriffskontroll-Liste von der Quelle der elektronischen Daten aus;
Speichern der aktualisierten Zugriffskontroll-Liste mit den im Datenarchiv gespeicherten elektronischen Daten; und
Speichern eines Beweises der aktualisierten Zugriffskontroll-Liste an der Quelle und bei jedem Benutzer, der zum Zugriff auf die elektronischen Daten im Archiv berechtigt ist.

15. Das Verfahren nach Anspruch 14, wobei der Schritt der Verifizierung des anfordernden Benutzers als Berechtigten das Auffinden des anfordernden Benutzers in der aktualisiertem Zugriffskontroll-Liste umfaßt.

16. Der Prozeß nach Anspruch 15, wobei dieser außerdem einen Schritt umfaßt, in dem die Richtigkeit der mit den elektronischen Daten im Datenarchiv gespeicherten aktualisierten Zugriffskontroll-Liste anhand des an der Quelle gespeicherten Beweises verifiziert wird, bevor die elektronischen Daten für den anfordernden Benutzer freigegeben werden.

17. Ein computerlesbarer Speicher zum Speichern der Instruktionen zur Verwendung bei der Ausführung eines der Verfahren nach Anspruch 7 bis 16 auf einem Computer.

Hierzu 7 Seite(n) Zeichnungen

Nummer: DE 199 60 977 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. Juli 2000

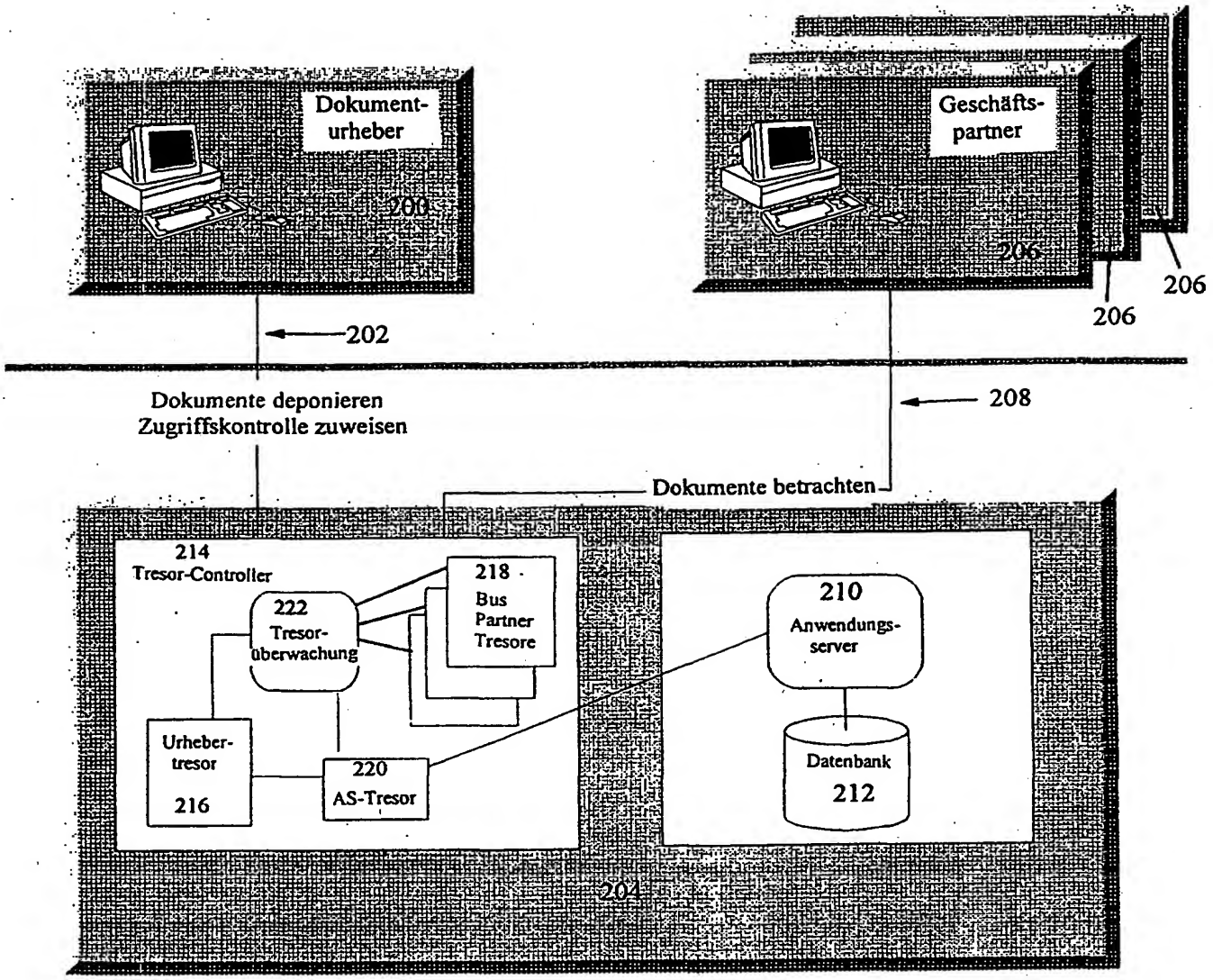


FIG. 2

Nummer: DE 199 60 977 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. Juli 2000

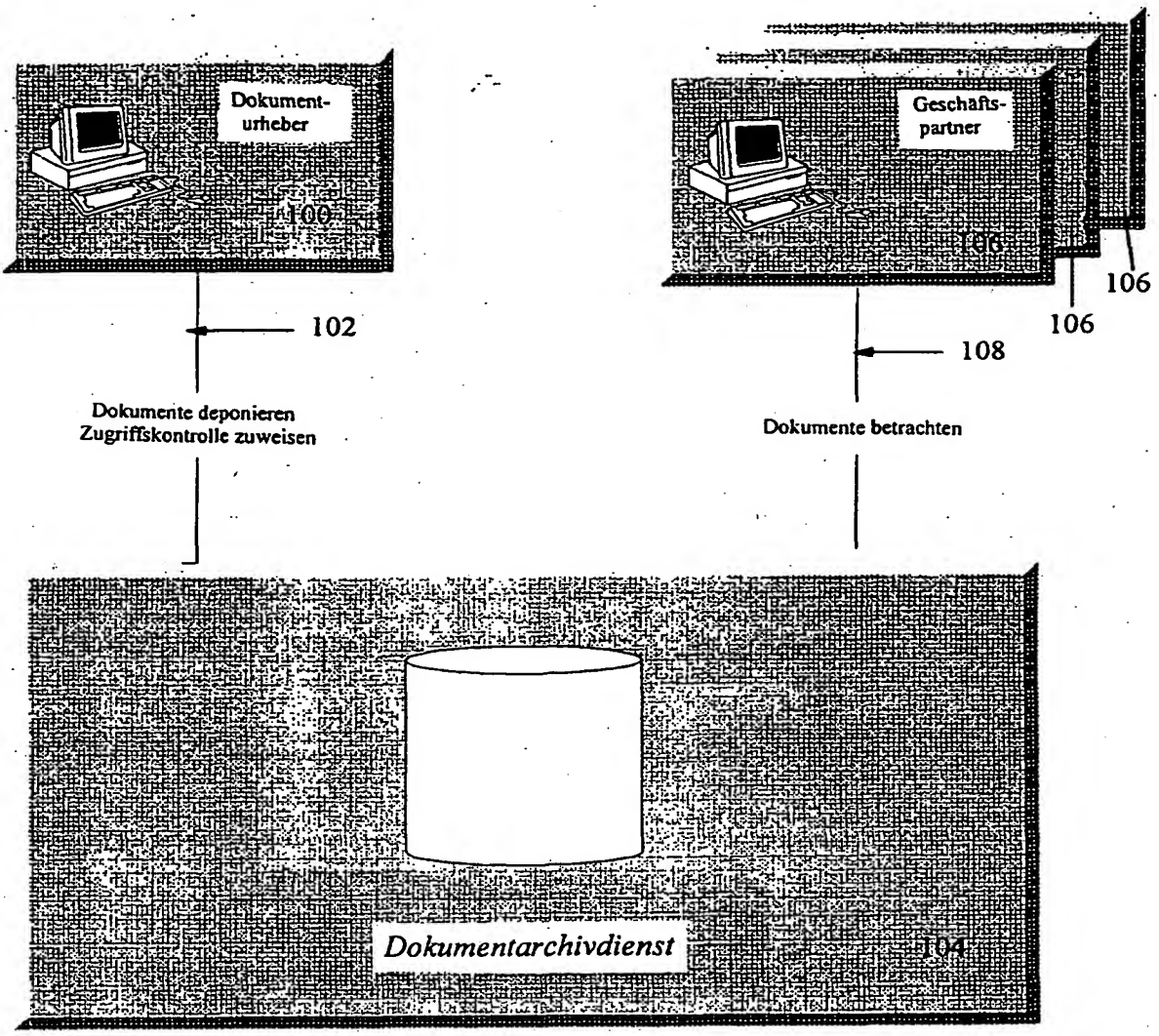


FIG. 1

STAND DER TECHNIK

Nummer: DE 199 60 977 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. Juli 2000

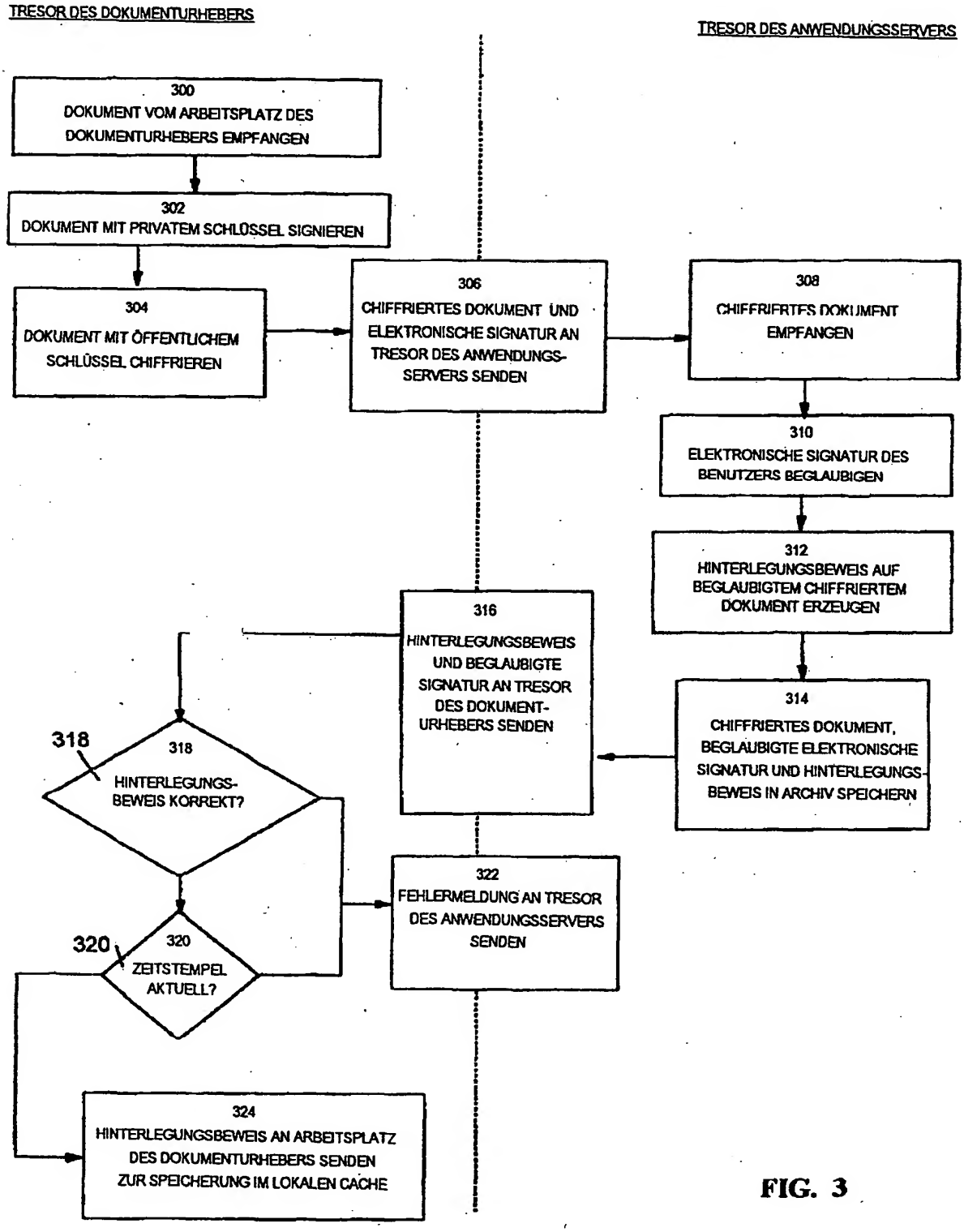


FIG. 3

Nummer: DE 199 60 977 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. Juli 2000

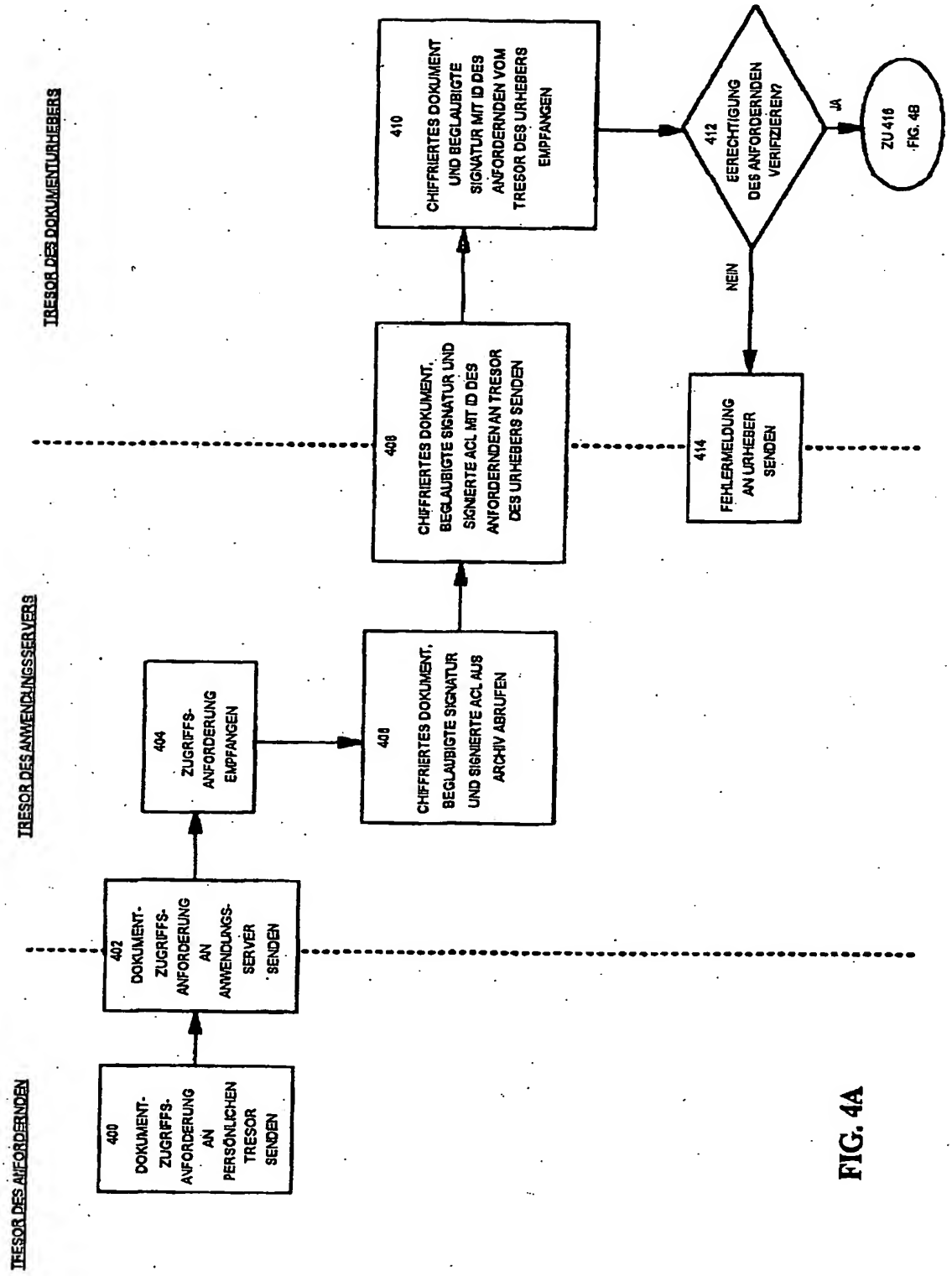


FIG. 4A

Nummer: DE 199 60 977 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. Juli 2000

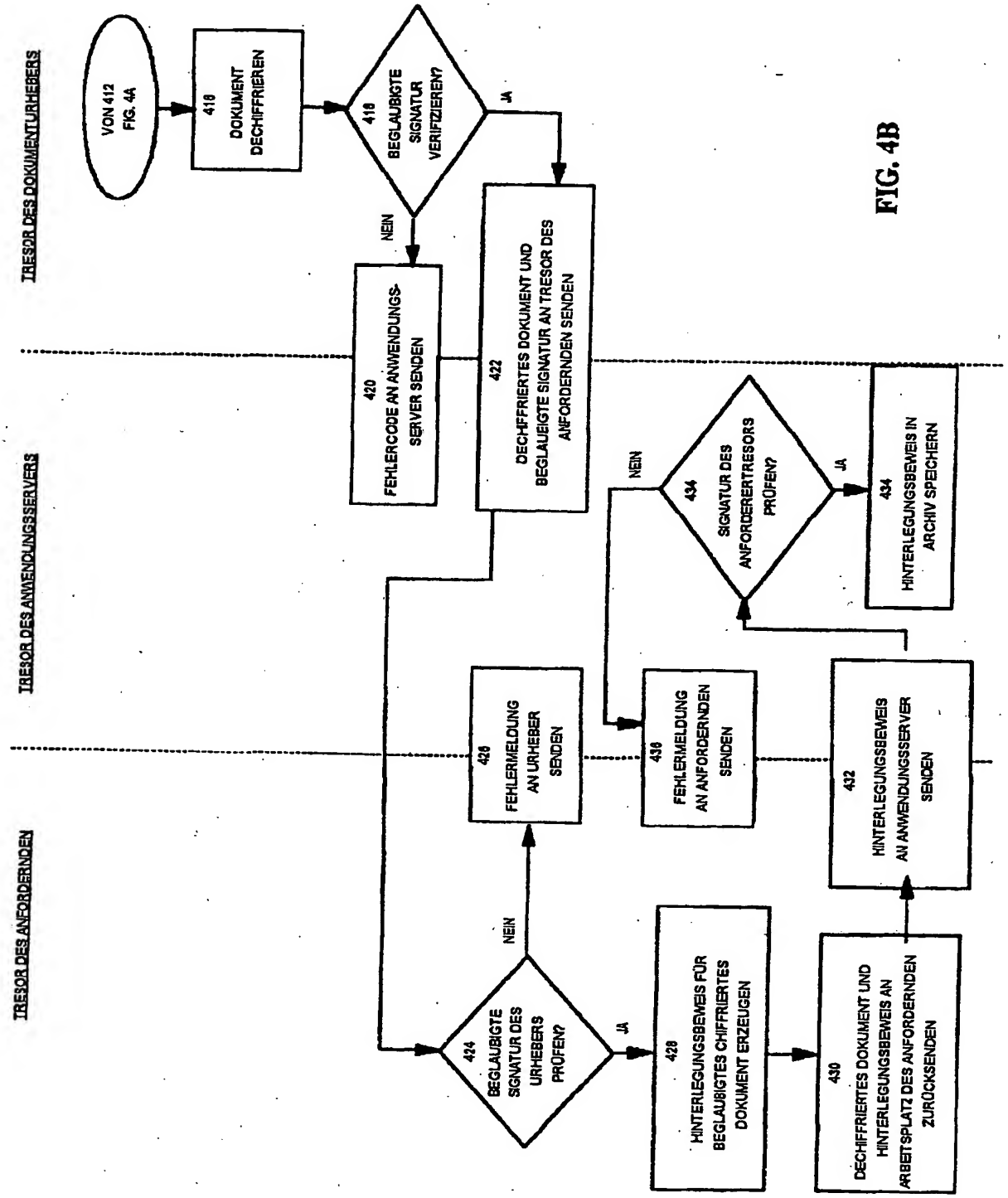
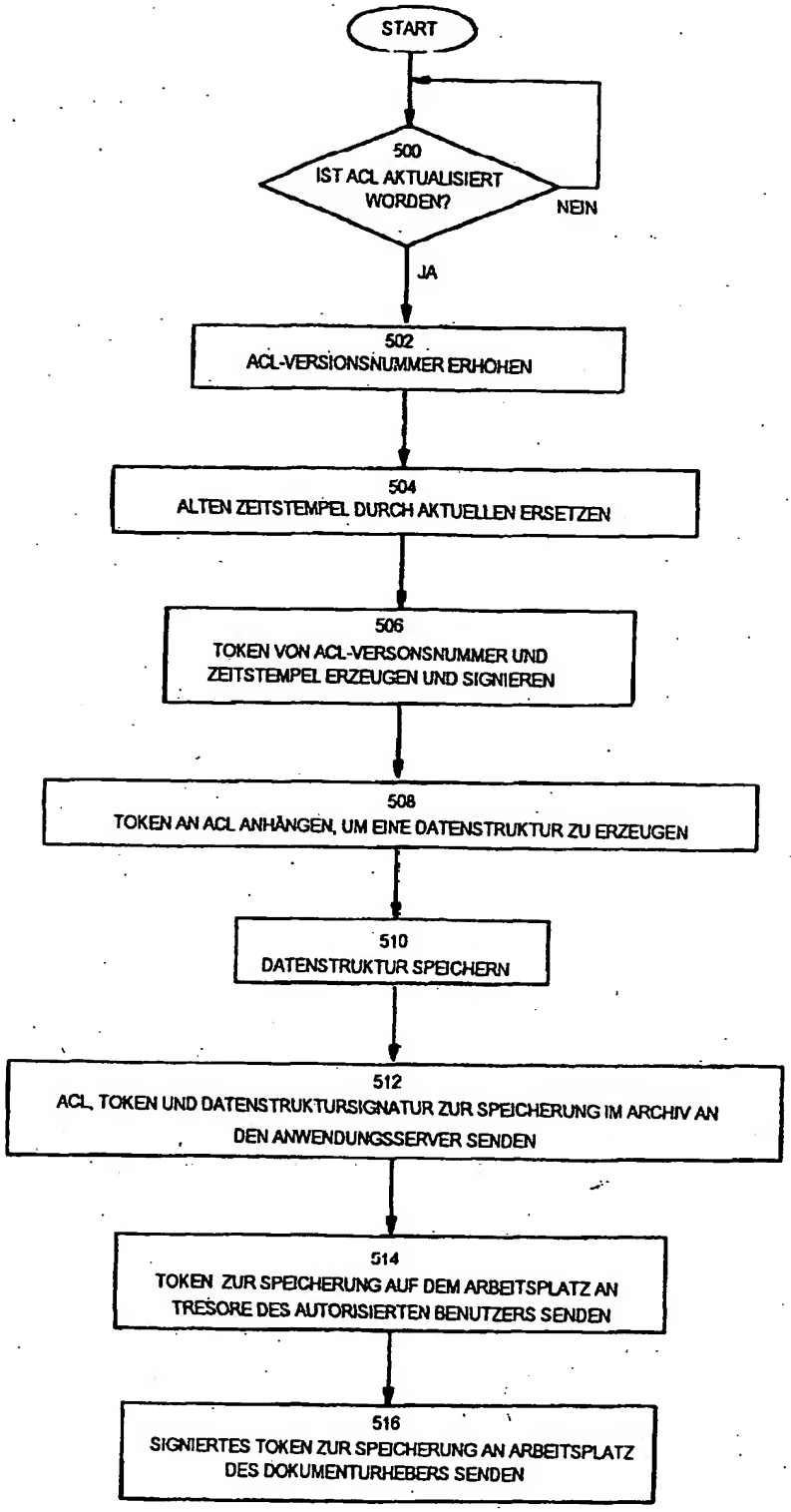


FIG. 4B

Nummer: DE 199 60 977 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. Juli 2000

FIG. 5



Nummer: DE 199 60 977 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. Juli 2000

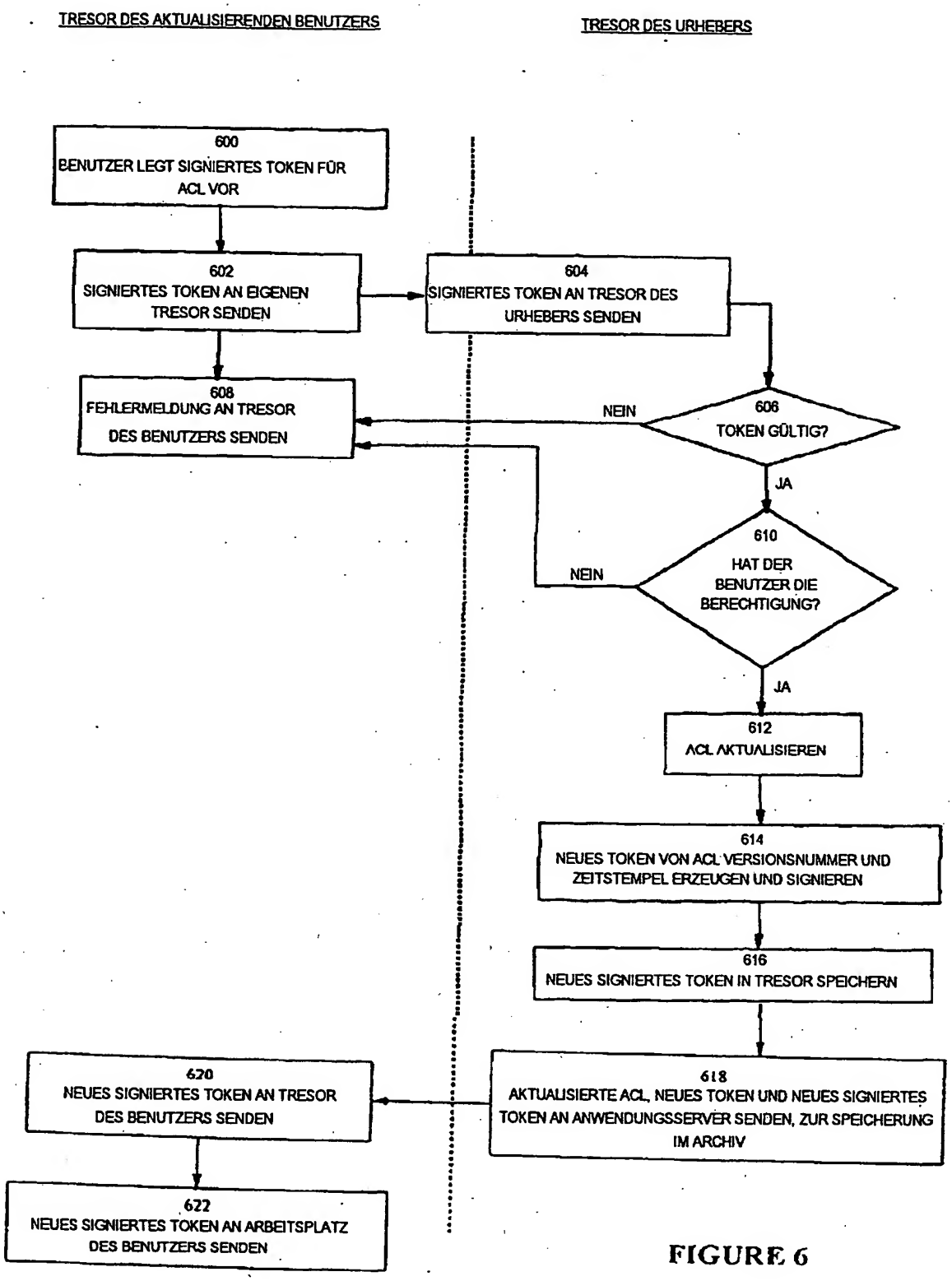
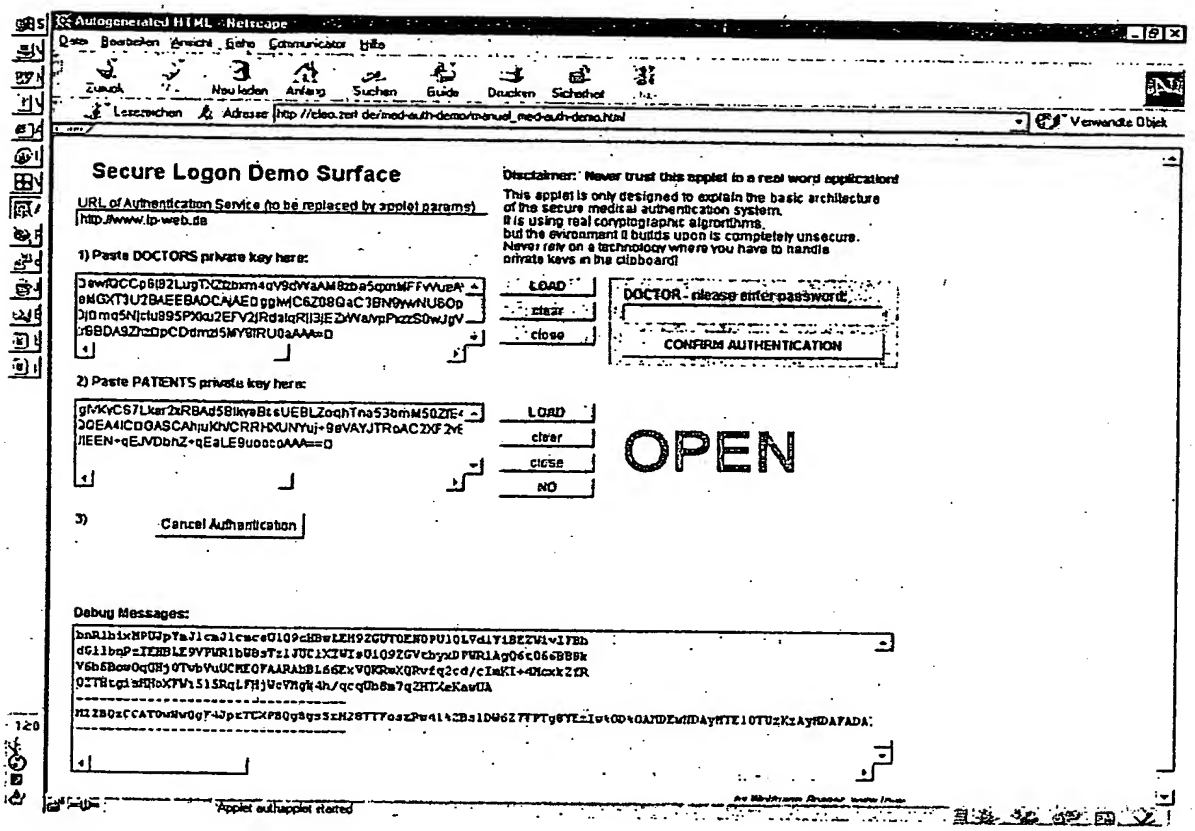


FIGURE 6

Nummer: DE 101 21 819 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 21. November 2002

Zeichnung 2 - Beispiel der Authentifizierungsoberfläche (Entwicklungsinstallation):



Nummer: DE 101 21 819 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 21. November 2002

Zeichnung 3 - Zertifikatsverwaltung in einem Standard-Browser: